

**UNITED STATES DISTRICT COURT**  
for the  
Western District of Washington

In the Matter of the Search of \_\_\_\_\_  
*(Briefly describe the property to be searched or identify the person by name and address)* \_\_\_\_\_ )  
 Information associated with \_\_\_\_\_ ) Case No. MJ19-028  
 john.w.alderon@outlook.com stored at premises \_\_\_\_\_ )  
 controlled by Microsoft Corp. \_\_\_\_\_ )

**APPLICATION FOR A SEARCH WARRANT**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A-1, incorporated herein by reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B-1, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- evidence of a crime;  
 contraband, fruits of crime, or other items illegally possessed;  
 property designed for use, intended for use, or used in committing a crime;  
 a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
Title 18, U.S.C., Sections 1343, 1344, and 1028A	Bank fraud, wire fraud, aggravated identity theft

The application is based on these facts:

- See Affidavit of SA Milas Howe, continued on the attached sheet.

Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

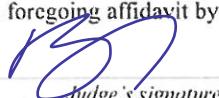
Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented:  by reliable electronic means; or:  telephonically recorded.

  
*Applicant's signature*

Milas Howe, Special Agent  
*Printed name and title*

- The foregoing affidavit was sworn to before me and signed in my presence, or  
 The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 1/18/19

  
*Judge's signature*

City and state: Seattle, Washington

Brian A. Tsuchida, Chief United States Magistrate Judge  
*Printed name and title*

## AFFIDAVIT

STATE OF WASHINGTON )  
 )  
COUNTY OF KING )

I, Milas Howe, being first duly sworn, depose and state as follows:

## **INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), assigned to the White Collar Crime Squad of the Seattle, Washington Headquarters Field Office. I have worked with the FBI since May 2017. I am responsible for investigating violations of federal statutes governing various types of white collar crime, including wire fraud, mail fraud, bank fraud, securities fraud, money laundering, and theft of government and public money. Prior to working for the FBI, I spent over ten years in the accounting industry working as both an internal and external auditor. I am a licensed Certified Public Accountant, Certified Fraud Examiner, and Certified Information Systems Auditor.

2. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

3. This affidavit does not detail each and every fact and circumstance I or others have learned during the course of this investigation. Furthermore, the investigation is ongoing, including the gathering and analysis of records. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits and instrumentalities of Wire Fraud, in violation of Title 18, United

1 States Code, Section 1343, Bank Fraud, in violation of Title 18, United States Code,  
2 Section 1344, and Aggravated Identity Theft, Title 18, United States Code, Section  
3 1028A, will be found on the SUBJECT EMAIL ACCOUNTS.

4 **SUMMARY OF THE FRAUDULENT SCHEME**

5 4. The target of this investigation is JOHN WILLIAM ALDERSON, who has  
6 a 2003 conviction for fraud in this District. The investigation has shown that, beginning  
7 in approximately 2014, ALDERSON devised and executed a scheme to defraud Austin  
8 McNamee. ALDERSON befriended McNamee and eventually became his romantic  
9 partner, giving ALDERSON access to McNamee's personal information. ALDERSON  
10 then fraudulently opened several credit cards in McNamee's name and ran up over  
11 \$100,000 in charges on those cards. ALDERSON also stole funds from an investment  
12 account belonging to McNamee. ALDERSON used email to further his fraud by (among  
13 other things) creating an email account in McNamee's name, and by sending fraudulent  
14 emails to McNamee.

15 **PLACES TO BE SEARCHED AND ITEMS TO BE SEIZED**

16 5. This affidavit is being submitted in support of an application for warrants  
17 authorizing the search of the following email accounts (collectively referred to as the  
18 "SUBJECT EMAIL ACCOUNTS":

- 19       a. [armcnamee98022@gmail.com](mailto:armcnamee98022@gmail.com)  
20       b. [alderson509@gmail.com](mailto:alderson509@gmail.com)  
21       c. [john.w.alderson@outlook.com](mailto:john.w.alderson@outlook.com), and  
22       d. [alderson98022@gmail.com](mailto:alderson98022@gmail.com).

23 6. The information associated with the [armcnamee98022@gmail.com](mailto:armcnamee98022@gmail.com),  
24 [alderson509@gmail.com](mailto:alderson509@gmail.com), and [alderson98022@gmail.com](mailto:alderson98022@gmail.com) accounts is stored at premises  
25 owned, maintained, controlled, or operated by Google Incorporated, an e-mail provider  
26 headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043, as  
27 further described in Attachment A, attached hereto and incorporated herein. The  
28 information associated with the [john.w.alderson@outlook.com](mailto:john.w.alderson@outlook.com) account is stored at

1 premises owned, maintained, controlled, or operated by Microsoft Corporation, an e-mail  
2 provider headquartered at 1 Microsoft Way, Redmond, Washington 98052, as further  
3 described in Attachment A-1, attached hereto and incorporated herein. Google and  
4 Microsoft are collectively referred to as "the Providers."

5       7. The information to be searched is described in the following paragraphs  
6 and in Attachments B and B-1. This affidavit is made in support of an application for a  
7 search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require  
8 the Providers to disclose to the government copies of the information (including the  
9 content of communications) further described at Attachments B and B-1. Upon receipt  
10 of the information described in Section I of Attachments B and B-1, government-  
11 authorized persons will review that information to locate the items described in Section II  
12 of the Attachments.

## SUMMARY OF THE INVESTIGATION

14        8. I have interviewed McNamee as part of this investigation. A lawyer  
15 representing McNamee has provided various records, including a written statement by  
16 McNamee that recounts McNamee's relationship with JOHN WILLIAM ALDERSON  
17 and explains how ALDERSON stole his identity and defrauded him.

18       9. According to McNamee, he first met ALDERSON in October of 2014,  
19 after ALDERSON contacted him through an online dating service. McNamee and  
20 ALDERSON initially became friends, and later became romantic partners. ALDERSON  
21 moved into McNamee's Seattle home in the summer of 2015.

22        10. I have seen court records showing that ALDERSON was convicted of wire  
23 fraud and social security fraud in this District in case number CR03-246L. In that case,  
24 ALDERSON pled guilty and admitted to a variety of fraudulent schemes, including  
25 impersonating an art broker and defrauding dealers by purchasing art with non-sufficient  
26 funds checks. On November 7, 2003, ALDERSON was sentencing to 41 months of  
27 imprisonment. ALDERSON, an attorney, was also disbarred in 2003 for writing \$21,550  
28 in unauthorized checks from the account of a business run by his father and uncle.

1     ALDERSON stole the checks from his parents' home and signed his father's name to the  
 2 checks. ALDERSON's father covered the loss to the business by paying \$21,550 of his  
 3 own money to the business. According to McNamee, ALDERSON did not tell  
 4 McNamee about his conviction or his disbarment.

5         11. According to McNamee, when he was getting to know ALDERSON,  
 6 ALDERSON lied to him about various things. ALDERSON presented himself as a  
 7 wealthy person who needed nothing financially from McNamee, and in fact was eager to  
 8 share his wealth with McNamee. From my training and experience, I know that con  
 9 artists will often pose as wealthy people, in order to put their victims at ease and hide  
 10 their true financial motives. This deception is often an integral part of a fraudulent  
 11 scheme. Con artists will often also use deception and manipulation to gain the trust and  
 12 affection of their intended victims, with the goal of inducing the victims to give the con  
 13 artists access to their money, property, and personal and financial information.

14         12. According to McNamee, ALDERSON claimed that he had been sexually  
 15 abused by a relative. ALDERSON claimed to have hired a lawyer, "Attorney A," who  
 16 was negotiating a settlement of the abuse claims with a lawyer representing his relative,  
 17 "Attorney B."

18         13. On January 28, 2015, ALDERSON (using the email account  
 19 [alderson509@gmail.com](mailto:alderson509@gmail.com)) forwarded emails to McNamee that purportedly came from  
 20 ALDERSON's lawyer, Attorney A.<sup>1</sup> I have seen these emails. The emails showed  
 21 Attorney A proposing a \$345,000 settlement to Attorney B, the lawyer for ALDERSON's  
 22 relative. On April 2, 2015, ALDERSON emailed McNamee (using the email address  
 23 [john.w.alderson@outlook.com](mailto:john.w.alderson@outlook.com)) and claimed that he had "signed the settlement agreement  
 24 today." As part of this same email, ALDERSON forwarded an email purportedly sent to  
 25 him by Attorney A, in which Attorney A appeared to ask if ALDERSON had signed the  
 26 settlement papers.

27 \_\_\_\_\_  
 28 <sup>1</sup> I will refer to all of the unnamed attorneys as if they are men, regardless of their real gender.

1       14. My investigation has shown that the emails from and between Attorney A  
 2 and Attorney B were forged. I have interviewed Attorney B. Attorney B did not  
 3 remember ever dealing with Attorney A, or receiving an email from Attorney A.  
 4 Attorney B said that he had never represented ALDERSON's relative in a sex assault  
 5 matter – indeed, Attorney B said that he had never handled a sex assault case in his entire  
 6 career as an attorney. Attorney B had done legal work for ALDERSON's family, which  
 7 may be how ALDERSON came across his name.

8       15. ALDERSON also claimed that he wanted McNamee to have power of  
 9 attorney, with full control of ALDERSON's finances and property, in case ALDERSON  
 10 became ill. ALDERSON claimed to have suffered several bouts of cancer in the past.  
 11 On August 27, 2015, ALDERSON (using the email address  
 12 [john.w.alderson@outlook.com](mailto:john.w.alderson@outlook.com)) forwarded an email to McNamee. I have seen this email.  
 13 The email (also dated August 27, 2015) was purportedly from "Attorney C," who worked  
 14 at a prominent Seattle law firm, to ALDERSON. In the email, Attorney C said that  
 15 Attorney C had prepared a draft power of attorney for ALDERSON at ALDERSON's  
 16 request. Attorney C said that it had been "too long" since Attorney C and ALDERSON  
 17 saw one another, and suggested having lunch the following week. Attached to the email  
 18 from Attorney C was an unsigned durable power of attorney giving McNamee "full  
 19 power and authority to manage and conduct" ALDERSON's affairs.

20       16. My investigation has shown that the August 27, 2015, email purportedly  
 21 sent by Attorney C to ALDERSON was fraudulent. I interviewed Attorney C and  
 22 showed him a copy of the August 27, 2015, email and attachment that he had purportedly  
 23 sent. Attorney C said that he had not sent that email. Attorney C said that he did not  
 24 know ALDERSON and had never represented ALDERSON. Attorney C said that the  
 25 signature block on the email did not match the signature block used by Attorney C.  
 26 Attorney C said that he had never drafted the power of attorney attached to the email, and  
 27 that he would not have drafted a power of attorney in that format. Attorney C confirmed  
 28 that, for many years, he had done legal work for an entity that employed McNamee.

AFFIDAVIT OF SA MILAS HOWE  
 USAO #2018R001185

UNITED STATES ATTORNEY  
 700 STEWART STREET, SUITE  
 5220  
 SEATTLE, WASHINGTON 98101  
 (206) 553-7970

1 From my investigation, I know that ALDERSON briefly worked (or contracted with) that  
2 same entity, which may be how ALDERSON came across Attorney C's name.

3       17. According to McNamee, after gaining McNamee's trust and affection – as  
4 well as access to McNamee's personal identifying information – ALDERSON stole  
5 McNamee's identity and used it to open several credit cards. According to McNamee, in  
6 2016 and 2017, ALDERSON opened multiple credit cards using McNamee's name or  
7 personal information, and ran up charges of over \$100,000 on those cards. According to  
8 McNamee, ALDERSON created an email account in McNamee's name --  
9 [armcnamee98022@gmail.com](mailto:armcnamee98022@gmail.com) – and used that account to communicate with credit card  
10 vendors. McNamee claimed that he did not know that ALDERSON had opened these  
11 credit cards using his name or personal information.

12       18. According to McNamee, he learned that ALDERSON had stolen his  
13 identity in April of 2017. At that time, two of McNamee's friends – N.D. and A.F. – told  
14 McNamee about ALDERSON's prior conviction. ALDERSON had sued A.F. in a  
15 dispute over a business that ALDERSON and A.F. were involved in. ALDERSON had  
16 obtained a default judgment against A.F in King County Superior Court. According to  
17 A.F., the default judgment had been obtained by fraud, as ALDERSON or his  
18 representatives had filed one or more false documents with the court claiming that A.F.  
19 had been served with a pleading, when in fact A.F. had not been served. After A.F.  
20 proved that the certificate of service was fraudulent, the court vacated the default  
21 judgment.

22       19. According to McNamee, after he learned about ALDERSON's history, he  
23 searched ALDERSON's wallet while ALDERSON slept. McNamee found multiple  
24 credit cards in McNamee's name. McNamee said that he had not known about these  
25 credit cards.

26  
27  
28

AFFIDAVIT OF SA MILAS HOWE  
USAO #2018R001185

UNITED STATES ATTORNEY  
700 STEWART STREET, SUITE  
5220  
SEATTLE, WASHINGTON 98101  
(206) 553-7970

1       20. I have obtained records for a US Bank credit card with an account number  
 2 ending in -8960 (later changed to -6488).<sup>2</sup> US Bank is a financial institution as defined in  
 3 Title 18, United States Code, Section 20. McNamee has identified this as one of the  
 4 accounts that ALDERSON fraudulently opened in his name, incurring over \$3,000 in  
 5 charges. The records show that the application for the credit card was submitted over the  
 6 internet on December 19, 2016, in McNamee's name. The email address on the  
 7 application was [armcnamee98022@gmail.com](mailto:armcnamee98022@gmail.com) and the phone number was 360-367-1724.  
 8 That same phone number is listed as ALDERSON's phone number on a copy of his  
 9 resume provided to investigators by McNamee. After learning of the card's existence,  
 10 McNamee contacted US Bank to report that the card had been opened fraudulently. On  
 11 May 18, 2017, a US Bank fraud investigator wrote to McNamee to confirm that the bank  
 12 had completed its identity theft investigation and would not hold McNamee liable for any  
 13 charges or fees.

14       21. Records for the -8960 account show a charge on April 10, 2017, for  
 15 \$2,161.89 at the Center of Plastic Surgery in Bellevue, Washington. According to US  
 16 Bank, the transaction originated in the merchant state of Washington, was transmitted to  
 17 Visa located in California, and then returned to Washington.

18       22. According to McNamee, ALDERSON also fraudulently transferred money  
 19 out of McNamee's investment account by gaining access to the account and changing the  
 20 contact information to ALDERSON's own information.

21       23. I have also seen an invoice sent to McNamee and his employer from  
 22 Bonham's, a London, England business. The invoice, dated May 2, 2017, was for a  
 23 March 14, 2017, transaction in the amount of £3,640 British Pounds. As with the Capital  
 24 One application, the email address on the invoice was [armcnamee98022@gmail.com](mailto:armcnamee98022@gmail.com) and  
 25 the phone number was 360-367-1724 (the phone number listed for ALDERSON on his  
 26 resume). McNamee claims that he never made this purchase, and that it was a fraudulent  
 27

---

28       2 I am continuing to obtain and review financial records.

1 transaction committed by ALDERSON. Attorneys representing McNamee's employer  
 2 disputed the charge with Bonham's, and I have seen correspondence reflecting that  
 3 Bonham's cancelled the transaction.

4       24. According to McNamee, ALDERSON also used the  
 5 [alderson98022@gmail.com](mailto:alderson98022@gmail.com) email address in furtherance of the fraud. McNamee  
 6 identified a Bank of America (Alaska Airlines) Visa card ending in -6032 that  
 7 ALDERSON fraudulently obtained by applying for it in McNamee's name on January  
 8 12, 2017. According to McNamee, ALDERSON ran up at least \$19,000 in charges on  
 9 this credit card. I have seen correspondence from Bank of America stating that it would  
 10 not hold McNamee responsible for the charges on account of fraud. According to  
 11 McNamee, ALDERSON used the [alderson98022@gmail.com](mailto:alderson98022@gmail.com) for this account.  
 12 McNamee has provided investigators with a photograph he took of ALDERSON's cell  
 13 phone (after McNamee learned of ALDERSON's scheme) showing a January 31, 2017,  
 14 email from Bank of America to [alderson98022@gmail.com](mailto:alderson98022@gmail.com) regarding the -6032 account.  
 15 According to McNamee he also found evidence that ALDERSON has used the  
 16 [alderson98022@gmail.com](mailto:alderson98022@gmail.com) to fraudulently apply for a credit card in ALDERSON's  
 17 father's name.

18       25. My investigation has uncovered evidence showing that, besides the  
 19 fraudulent credit cards in McNamee's name, ALDERSON was committing many other  
 20 frauds, such as: falsely reporting that airlines had lost valuables in his luggage, falsely  
 21 disputing credit card purchases as "fraudulent" when in fact ALDERSON made the  
 22 purchases, and refusing to pay for purchases that ALDERSON made for vendors by  
 23 falsely claiming identity theft. The evidence suggests that ALDERSON may have been  
 24 defrauding antique and art dealers, similar to the fraud he was convicted for in 2003.  
 25 ALDERSON is also pending trial in King County Superior Court for retail theft from his  
 26 employer. I have seen a written statement ALDERSON made to the Seattle Police  
 27 Department in that case on December 9, 2017, in which he admits to doing "14  
 28 fraud[ulent] returns for \$18,291."

AFFIDAVIT OF SA MILAS HOWE  
 USAO #2018R001185

UNITED STATES ATTORNEY  
 700 STEWART STREET, SUITE  
 5220  
 SEATTLE, WASHINGTON 98101  
 (206) 553-7970

1

2                   **PROBABLE CAUSE REGARDING THE SUBJECT EMAIL**

3                   **ACCOUNTS**

4         26. As set forth above, there is probable cause to believe that evidence of the  
 5 offenses of wire fraud, bank fraud, and identity theft may be found in the SUBJECT  
 6 EMAIL ACCOUNTS. The fraudulent scheme, by its nature, relied heavily upon email.  
 7 I know, from my training and experience, that people involved in fraud often use email in  
 8 various ways to further their schemes, including but not limited to email communications  
 9 between schemers, and transmission of false or misleading information to victims.

10                  **BACKGROUND REGARDING THE PROVIDERS' SERVICES**

11         27. In my training and experience, I have learned that the Providers provides a  
 12 variety of on-line services, including electronic mail ("e-mail") access, to the general  
 13 public.

14         28. Subscribers obtain an account by registering with the Providers. When  
 15 doing so, e-mail providers like the Providers ask the subscriber to provide certain  
 16 personal identifying information. This information can include the subscriber's full  
 17 name, physical address, telephone numbers and other identifiers, alternative e-mail  
 18 addresses, and, for paying subscribers, means and source of payment (including any  
 19 credit or bank account number). In my training and experience, such information may  
 20 constitute evidence of the crimes under investigation because the information can be used  
 21 to identify the account's user or users, and to help establish who has dominion and  
 22 control over the account.

23         29. E-mail providers typically retain certain transactional information about the  
 24 creation and use of each account on their systems. This information can include the date  
 25 on which the account was created, the length of service, records of log-in (i.e., session)  
 26 times and durations, the types of service utilized, the status of the account (including  
 27 whether the account is inactive or closed), the methods used to connect to the account  
 28 (such as logging into the account via a Provider's website), and other log files that reflect

1 usage of the account. In addition, e-mail providers often have records of the Internet  
 2 Protocol address (“IP address”) used to register the account and the IP addresses  
 3 associated with particular logins to the account. Because every device that connects to  
 4 the Internet must use an IP address, IP address information can help to identify which  
 5 computers or other devices were used to access the e-mail account, which can help  
 6 establish the individual or individuals who had dominion and control over the account

7       30. In general, an e-mail that is sent to the Providers’ subscribers is stored in  
 8 the subscriber’s “mail box” on the Providers’ servers until the subscriber deletes the e-  
 9 mail. If the subscriber does not delete the message, the message can remain on the  
 10 Providers’ servers indefinitely. Even if the subscriber deletes the e-mail, it may continue  
 11 to be available on the Providers’ servers for a certain period of time.

12       31. When the subscriber sends an e-mail, it is initiated at the user’s computer,  
 13 transferred via the Internet to the Providers’ servers, and then transmitted to its end  
 14 destination. The Providers often maintains a copy of the e-mail sent. Unless the sender  
 15 of the e-mail specifically deletes the e-mail from the Providers’ server, the e-mail can  
 16 remain on the system indefinitely. Even if the sender deletes the e-mail, it may continue  
 17 to be available on the Providers’ servers for a certain period of time.

18       32. A sent or received e-mail typically includes the content of the message,  
 19 source and destination addresses, the date and time at which the e-mail was sent, and the  
 20 size and length of the e-mail. If an e-mail user writes a draft message but does not send  
 21 it, that message may also be saved by the Providers but may not include all of these  
 22 categories of data.

23       33. In some cases, e-mail account users will communicate directly with an e-  
 24 mail service provider about issues relating to the account, such as technical problems,  
 25 billing inquiries, or complaints from other users. E-mail providers typically retain  
 26 records about such communications, including records of contacts between the user and  
 27 the provider’s support services, as well records of any actions taken by the provider or  
 28 user as a result of the communications. In my training and experience, such information

1 may constitute evidence of the crimes under investigation because the information can be  
 2 used to identify the account's user or users.

3                   **PAST EFFORTS TO OBTAIN THIS EVIDENCE**

4         34. This evidence has not been previously available to me or other agents, apart  
 5 from subscriber information records.

6                   **PROTOCOL FOR SORTING SEIZABLE ELECTRONICALLY**  
 7                   **STORED INFORMATION**

8         35. In order to ensure that agents are limited in their search only to the e-mail  
 9 account specifically sought (and any attachments, stored instant messages, stored voice  
 10 messages, and photographs associated therewith); in order to protect the privacy interests  
 11 of other third parties who have accounts at the Providers; and in order to minimize  
 12 disruptions to normal business operations of the Providers; this application seeks  
 13 authorization to permit agents and employees of the Providers to assist in the execution of  
 14 the warrants, as follows: (See: Title 18, United States Code, Section 2703(g)).

15         36. The search warrants will be presented to the Providers, with direction that  
 16 they identify and isolate the e-mail accounts and associated records described in Section I  
 17 of Attachments B and B-1.

18         37. The Providers will also be directed to create an exact duplicate in electronic  
 19 form of the e-mail accounts and records specified in Section I of Attachments B and B-1,  
 20 including an exact duplicate of the content of all e-mail messages stored in the specified  
 21 e-mail account.

22         38. The Providers shall then provide exact digital copies of the content of the  
 23 subject e-mail accounts, as well as all other records associated with the account, to me, or  
 24 to any other agent of the FBI. Once the digital copies have been received from the  
 25 Providers, that copy will, in turn, be forensically imaged and only that image will be  
 26 reviewed and analyzed to identify communications and other data subject to seizure  
 27 pursuant to Section II of Attachments B and B-1. The original digital copies will be  
 28 sealed and maintained to establish authenticity, if necessary.

AFFIDAVIT OF SA MILAS HOWE  
 USAO #2018R001185

UNITED STATES ATTORNEY  
 700 STEWART STREET, SUITE  
 5220  
 SEATTLE, WASHINGTON 98101  
 (206) 553-7970

1       39. I, and/or other agents of the FBI will thereafter review the forensic images,  
 2 and identify from among that content those items that come within the items identified in  
 3 Section II to Attachments B and B-1, for seizure. I, and/or other agents of the FBI will  
 4 then copy those items identified for seizure to separate media for future use in the  
 5 investigation and prosecution. The forensic copy of the complete content of the e-mail  
 6 accounts will also then be sealed and retained by the FBI, and will not be unsealed absent  
 7 authorization of a Magistrate Judge of this Court, except for the purpose of duplication of  
 8 the entire image in order to provide it, as discovery, to a charged defendant.

9       40. Analyzing the data contained in the forensic image may require special  
 10 technical skills, equipment, and software. It could also be very time-consuming.  
 11 Searching by keywords, for example, can yield thousands of "hits," each of which must  
 12 then be reviewed in context by the examiner to determine whether the data is within the  
 13 scope of the warrant. Merely finding a relevant "hit" does not end the review process.  
 14 Keywords used originally need to be modified continuously, based on interim results.  
 15 Certain file formats, moreover, do not lend themselves to keyword searches, as keywords  
 16 search text, and many common electronic mail, database, and spreadsheet applications,  
 17 (which may be attached to e-mail,) do not store data as searchable text. The data is  
 18 saved, instead, in proprietary non-text format. And, as the volume of storage allotted by  
 19 service providers increases, the time it takes to properly analyze recovered data increases,  
 20 as well. Consistent with the foregoing, searching the recovered data for the information  
 21 subject to seizure pursuant to this warrant may require a range of data analysis techniques  
 22 and may take weeks or even months.

23       41. Based upon my experience and training, and the experience and training of  
 24 other agents with whom I have communicated, it is necessary to review and seize all  
 25 electronic mails, chat logs and documents, that identify any users of the subject account  
 26 and any electronic mails sent or received in temporal proximity to incriminating e-mails  
 27 that provide context to the incriminating communications.

28

AFFIDAVIT OF SA MILAS HOWE  
 USAO #2018R001185

UNITED STATES ATTORNEY  
 700 STEWART STREET, SUITE  
 5220  
 SEATTLE, WASHINGTON 98101  
 (206) 553-7970

42. All forensic analysis of the image data will employ only those search protocols and methodologies reasonably designed to identify and seize the items identified in Section II of Attachments B and B-1 to the warrant.

4       43. Records and files that could otherwise be obtained by subpoena shall  
5 remain available, in their entirety, to investigating agents and prosecutors for the duration  
6 of the investigation and prosecution. These include the name and address of the  
7 subscriber to or customer of the service; local and long distance telephone connection  
8 records; records of session times and durations; length of service and types of services  
9 utilized; telephone or instrument number or other subscriber number or identity,  
10 including any temporarily assigned network address; and means and source of payment,  
11 including any credit card and bank account numbers.

12        44. If in the course of their efforts to identify and segregate evidence of the  
13 items specified in Section II to Attachments B and B-1, law enforcement agents or  
14 analysts discover items outside of the scope of the warrant that are evidence of other  
15 crimes, that data/evidence will not be used in any way unless it is first presented to a  
16 Magistrate Judge of this District and a new warrant is obtained to seize that data, and/or  
17 to search for other evidence related to it. In the event a new warrant is authorized, the  
18 government may make use of the data then seized in any lawful manner.

## **REQUEST FOR NON-DISCLOSURE AND SEALING**

20       45. The government requests, pursuant to the preclusion of notice provisions of  
21 Title 18, United States Code, Section 2705(b), that the Providers be ordered not to notify  
22 any person (including the subscriber or customer to which the materials relate) of the  
23 existence of this warrant for such period as the Court deems appropriate. The  
24 government submits that such an order is justified because notification of the existence of  
25 this Order would seriously jeopardize the ongoing investigation. Such a disclosure would  
26 give the subscriber an opportunity to destroy evidence, change patterns of behavior,  
27 notify confederates, or flee or continue his flight from prosecution.

46. It is further respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. This is an ongoing investigation, and the targets do not know the details of what investigators have learned and what evidence has been gathered. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness by resulting in the flight of targets, the destruction of evidence, or the intimidation or influencing of witnesses.

## **CONCLUSION**

47. Based on the forgoing, I request that the Court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated,” per 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Accordingly, by this Affidavit and Warrant I seek authority for the government to search all of the items specified in Section I, Attachments B and B-1 (attached hereto and incorporated by reference herein) to the Warrant, and specifically to seize all of the data, documents and records that are

11

21 //

22 //

23 //

24 //

25 //

26 //

27 //

**AFFIDAVIT OF SA MILAS HOWE  
USAO #2018R001185**

UNITED STATES ATTORNEY  
700 STEWART STREET, SUITE  
5220  
SEATTLE, WASHINGTON 98101  
(206) 553-7970

1 identified in Section II to those same Attachments.  
2  
3  
4

MILAS HOWE  
Special Agent,  
Federal Bureau of Investigation

8 The above-named agent provided a sworn statement attesting to the truth of the  
9 contents of the foregoing affidavit on the 18 day of Jan, 2019.

Brian A. Tsuchida

11  
12  
13 BRIAN A. TSUCHIDA  
14 Chief United States Magistrate Judge  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

AFFIDAVIT OF SA MILAS HOWE  
USAO #2018R001185

UNITED STATES ATTORNEY  
700 STEWART STREET, SUITE  
5220  
SEATTLE, WASHINGTON 98101  
(206) 553-7970

1                   **ATTACHMENT A-1**

2                   **Account to be Searched**

3                   This warrant applies to information associated with the email account  
4                   john.w.alderon@outlook.com that is stored at premises owned, maintained, controlled,  
5                   or operated by Microsoft Corporation, an e-mail provider headquartered at 1 Microsoft  
6                   Way, Redmond, Washington 98052.

7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

AFFIDAVIT OF SA MILAS HOWE  
USAO #2018R001185

UNITED STATES ATTORNEY  
700 STEWART STREET, SUITE  
5220  
SEATTLE, WASHINGTON 98101  
(206) 553-7970

**ATTACHMENT B-1**

**I. Section I - Information to be disclosed by Microsoft Corporation, for search:**

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of Microsoft Corporation (“Microsoft”), including any e-mails, records, files, logs, or information that has been deleted but is still available to Microsoft, Microsoft is required to disclose the following information to the government for each account or identifier listed in Attachment A-1:

b. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. The types of service utilized:

e. All records pertaining to communications between Microsoft and any person regarding the account, including contacts with support services and records of actions taken.

f. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

g. All subscriber records associated with the specified account including lists of all related accounts, any contact lists, and content and/or preserved data

1                   **II. Section II - Information to be seized by the government**

2                   All information described above in Section I that constitutes fruits, contraband,  
 3 evidence and instrumentalities of violations of Bank Fraud, in violation of Title 18,  
 4 United States Code, Section 1344, Wire Fraud, in violation of Title 18, United States  
 5 Code, Section 1343, and Identity Theft, in violation of Title 21, United States Code,  
 6 Section 1028A, including, for the account or identifier listed on Attachment A-1,  
 7 information pertaining to the following matters:

- 8                   h.        Communications or material related to Austin McNamee;
- 9                   b.        Communications, or material related to credit cards, banks, or  
 10 financial institutions;
- 11                  c.        Communications or material related to purchases from vendors of  
 12 good or services, including disputed purchases;
- 13                  d.        Communications or material related to lost property in the care of  
 14 airlines;
- 15                  f.        Personal identifying information, including but not limited to Social  
 16 Security numbers, dates of birth, account numbers, and passwords;
- 17                  g.        All messages, documents, and profile information, attachments, or  
 18 other data that serves to identify any persons who use or access the account  
 19 specified, or who exercise in any way any dominion or control over the  
 20 specified account;
- 21                  h.        Any address lists or buddy/contact lists associated with the specified  
 22 account;
- 23                  i.        All messages, documents and profile information, attachments, or  
 24 other data that otherwise constitutes evidence, fruits, or instrumentalities of  
 25 violations of Bank Fraud, in violation of Title 18, United States Code,  
 26 Section 1344, Wire Fraud, in violation of Title 18, United States Code,  
 27 Section 1343, and Identity Theft, in violation of Title 21, United States  
 28 Code, Section 1028A .

- 1           j. All subscriber records associated with the specified account,  
2           including name, address, local and long distance telephone connection  
3           records, or records of session times and durations, length of service  
4           (including start date) and types of service utilized, telephone or instrument  
5           number or other subscriber number or identity, including any temporarily  
6           assigned network address, and means and source of payment for such  
7           service) including any credit card or bank account number;
- 8
- 9           k. All log records, including IP address captures, associated with the  
10          specified account; and
- 11
- 12          l. Any records of communications between the email service provider,  
13          and any person about issues relating to the account, such as technical  
14          problems, billing inquiries, or complaints from other users about the  
15          specified account. This to include records of contacts between the  
16          subscriber and the provider's support services, as well as records of any  
17          actions taken by the provider or subscriber as a result of the  
18          communications.
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28

AFFIDAVIT OF SA MILAS HOWE  
USAO #2018R001185

UNITED STATES ATTORNEY  
700 STEWART STREET, SUITE  
5220  
SEATTLE, WASHINGTON 98101  
(206) 553-7970